© 2022 The authors and IOS Press.

This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).

doi:10.3233/SHT1220671

Data Protection in Healthcare Research: Medical Students' Knowledge and Behavior

Marialida FARAH^{a,1}, Samar HELOU^b, Pascal TUFENKJI^c and Elie EL HELOU^a

^a Faculty of Medicine, Saint Joseph University, Lebanon

^b Global Center for Medical Engineering and Informatics, Osaka University, Japan

^c National Institute of Communication & Informatics, Saint Joseph University, Lebanon

Abstract. Healthcare research involves handling personal health information. Information security policies are implemented in research institutions to ensure data subjects' rights but are not always respected due to researchers' neglect or unawareness. This paper is part of an action research project at Saint Joseph University in Lebanon aiming to increase researchers' compliance with the university's information security policy. An anonymous online questionnaire was administered to medical students to evaluate their knowledge and behavior regarding patient data handling in research projects. 38 responses were collected. Results show that most students collect patient data for research, and are frequently not aware of, and do not comply with, the existing information security policy. We also found correlations between low knowledge and non-compliant behaviors including clicking on links from unknown senders, leaving computers unattended, and sharing data insecurely. To address these issues, we plan to implement various Information Security Awareness interventions and compare their effectiveness.

Keywords. Data protection, information security, research, knowledge, behavior

1. Introduction

Healthcare research often requires collecting, storing, and sharing patient health data. Patient health data are sensitive personal information and need to be handled in a way that ensures patients' rights to information, control over their data, and privacy [1]. The General Data Protection Regulation (GDPR) has been established in the European Union to guide individuals and organizations handling sensitive personal information. The GDPR covers several data handling aspects and was adopted by institutions inside and outside of Europe including Saint Joseph University in Beirut, Lebanon [1, 2]. The existence of such regulations does not by itself guarantee the security of personal information. To this day, most data breach incidents prove to be the result of employees' neglect and failure to follow the institution's information security policies, procedures, and guidelines [3]. Neglect or failure to follow information security policies may be attributed to a lack of knowledge or awareness. The Knowledge-Attitude-Behavior (KAB) model has been used in several studies and highlights improvements in information security behavior among individuals after changes in their attitudes which

¹ Corresponding Author, Marialida Farah, E-mail: farah.marialida@gmail.com

may have resulted from improved knowledge [4]. Accordingly, Information Security Awareness (ISA) interventions are recommended to improve compliance with information security policies [3]. This work is part of an action research project at Saint Joseph University of Beirut, aiming to increase researchers' compliance with the university's information security policy. As a first step, we aim to evaluate medical students' current knowledge and behavior regarding patient data handling in medical research and assess the link between both factors. Medical students are targeted as they are the most junior researchers in the organization and may be the weakest link in the security chain. Based on the findings, we plan to design various ISA interventions and compare their effectiveness.

2. Methods

This study was approved by the institutional review board of Saint Joseph University of Beirut (USJ), Lebanon. We administered an anonymous online questionnaire to the 6th and 7th year medical students at the faculty of medicine at USJ. Students were invited to complete the questionnaire using internal mailing lists. We designed the questionnaire based on USJ's information security policy and the GDPR. The questionnaire included 10 multiple choice questions assessing students' general knowledge on personal information security, 13 questions on their data handling behavior using a 5-point Likert scale ranging from "0: Never" to "4: Always", one multiple choice question about the data sources used in their research, and three background questions. Each knowledge question was scored between "0: Completely wrong" and "10: Completely correct". A total knowledge score—ranging from 0 to 100—was calculated by summing the scores of the individual knowledge questions. Descriptive statistics were used to analyze the students' knowledge and behavior regarding personal information security measures. Spearman correlation was used to assess the knowledge-behavior relationship.

3. Results

38 responses were collected in February 2022. 26 students (68.4%) reported collecting patient health data for their research. 17 (44.7%) students collected patient health data from existing patient medical records, 12 (31.6%) from patients themselves, and 6 (15.8%) from patients' physicians.

3.1. Medical students' knowledge of personal information security measures

Students' total knowledge scores—scored over 100—were normally distributed (M = 31.9, SD = 17). The mean total knowledge score shows that students lack the necessary knowledge to securely handle patient data. Table 1 shows how the students performed on each knowledge question. In general, students had acceptable knowledge of only two personal information security measures: consent requirements i.e., consent must be freely given, specific, and can be revoked and common social engineering vectors i.e., phishing, smishing, impersonation, and vishing. On the other hand, students were least aware of the target of GDPR and how to report data breaches and inform subjects affected by these breaches.

	Correct	Partially correct	Wrong
Consent requirements	40%	60%	0%
Common social engineering vectors	32%	50%	18%
Protecting data on mobile devices	0%	61%	39%
Reacting to data breaches	21%	24%	55%
Subjects' privacy rights	13%	32%	55%
University's security policy	16%	26%	58%
Anonymization and pseudo-anonymization	13%	29%	58%
Informing subjects of data breaches	5%	21%	74%
Reporting data breaches	16%	0%	84%
Target of GDPR	8%	0%	92%

Table 1. Medical students' knowledge of the university's personal information security measures.

3.2. Medical students' compliance with personal information security measures

Table 2 shows students' data handling behavior and how their behaviors correlate with their knowledge scores. The results show that students do not always comply with the information policy. Significant correlations were found between students' knowledge and three non-compliant data handling behaviors. Students with lower knowledge scores reported higher frequencies of clicking on links in emails from unknown senders (ρ = -0.44, p = 0.005), leaving their laptops unattended in public spaces (ρ = -0.39, p = 0.014), sharing sensitive patient information with their colleagues via hard copies and emails (ρ = -0.36, p = 0.025). Surprisingly, students with higher knowledge scores reported using strong passwords less frequently for their work accounts (ρ = -0.34, p = 0.034).

Table 2. Medical students' compliance with the university's personal information security measures and its correlation with their knowledge score.

Compliant behaviors	Never	Rarely	Sometimes	Often	Always	Spearman ρ
1- Using a strong combination for work passwords	26%	18%	26%	13%	16%	-0.34 (p = 0.034)
2- Deleting sensitive patient data when no longer needed	18%	29%	13%	18%	21%	0.13 (p = 0.44)
3- Encrypting sensitive data that is collected and shared	34%	37%	13%	5%	11%	0.1 (p = 0.54)
4- Reporting a data breach or security incident when they occur	8%	18%	18%	16%	40%	-0.12 (p = 0.46)
5- Discarding sensitive printouts by shredding or destroying them	11%	21%	21%	24%	24%	0.17 (p = 0.3)
Non-Compliant behaviors	Never	Rarely	Sometimes	Often	Always	Spearman ρ
1- Storing sensitive patient data on personal mobile devices	16%	40%	26%	11%	8%	0.17 (p = 0.3)
2- Sharing work passwords with colleagues	42%	37%	21%	0%	0%	-0.25 (p = 0.12)
3- Clicking on links in emails from unknown senders	63%	18%	13%	5%	0%	-0.44 (p = 0.005)
4- Leaving laptop unattended in public spaces	40%	21%	26%	11%	3%	-0.39 (p = 0.014)
5- Sharing patient data with colleagues via hard copies/emails	66%	18%	13%	3%	0%	-0.36 (p = 0.025)
6- Staying logged in on work accounts with patient data	53%	29%	16%	3%	0%	-0.21 (p = 0.19)
7- Seeing patient data in insecure locations (on tables/desks)	24%	34%	21%	18%	3%	-0.04 (p = 0.82)
8- Writing passwords in insecure and easily accessible locations	55%	18%	26%	0%	0%	-0.24 (p = 0.15)

4. Discussion

Our results show that most medical students collect patients' data to conduct their research, but they lack knowledge of, and do not always comply with, the institution's security policies. Moreover, we found significant correlations between low knowledge and three non-compliant data handling behaviors. In this case, including information security courses in the curriculum, implementing ISA interventions, providing management support, and working on the institutions' security culture may prove helpful in improving students' knowledge and potentially their compliance [3]. However, it is unclear which ISA interventions are the most effective. Therefore, our future work includes implementing various ISA interventions and comparing their effectiveness.

Surprisingly, our results show that medical students with higher knowledge tend to use strong passwords less frequently for their work accounts which includes the hospital's EMR systems. This finding does not align with previous findings showing that using strong passwords is correlated with higher levels of cybersecurity knowledge [5]. This difference could be attributed to the work context: medical staff, working in the hospital, tend to share their accounts with other colleagues and use short passwords for convenience and speed when logging in and providing access to others when collaboration is needed. Since using easy passwords is common practice among the staff, knowledgeable students may be aware of their password's weakness and report it as such. Meanwhile, students with lower knowledge may overestimate their password's strength.

Finally, in this paper, we examined the relationship between knowledge and self-reported behavior which can be biased as people tend to respond in socially desirable ways. Therefore, further work is needed to evaluate students' real behavior in practice.

5. Conclusions

In our institution, although an information security policy exists, medical students' knowledge of the policy's content is low, and they do not always comply with it. Information security awareness interventions and the inclusion of information security courses in the medical curriculum are needed to improve students' knowledge. Moreover, since behavior is context-dependent, an in-depth examination of students' data handling behaviors is needed to understand other reasons for non-compliance.

References

- [1] Wirth FN, et al. Privacy-preserving data sharing infrastructures for medical research: systematization and comparison. BMC Medical Informatics and Decision Making. 2021;21(1):242.
- [2] Vlahou A, et al. Data sharing under the general data protection regulation: time to harmonize law and research ethics? Hypertension. 2021;77(4):1029-35.
- [3] Khando K, Gao S, Islam SM, Salman A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security. 2021;106:102267.
- [4] Parsons K, et al. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security. 2017;66:40-51.
- [5] Kennison SM, Jones IT, Spooner VH, Chan-Tin DE. Who creates strong passwords when nudging fails. Computers in Human Behavior Reports. 2021;4:100132.